Web **Share**
111U

Dual-Port ADSL2+
Modem/Router

User Guide

Atlantis Land

A02-RA111U(v1.5)_ME01 (v1.0 Mar 2009)

Atlantis Land

CE Mark Warning
In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

CE/EMC Restriction of Liability
The product described in this handbook was designed, produced and approved according to the EMC-regulations and is certified to be within EMC limitations.
If the product is used in an uncertified PC, the manufacturer undertakes no warranty in respect to the EMC limits. The described product in this handbook was constructed, produced and certified so that the measured values are within EMC limitations. In practice and under special circumstances, it may be possible, that the product may be outside of the given limits if it is used in a PC that is not produced under EMC certification. It is also possible in certain cases and under special circumstances, which the given EMC peak values will become out of tolerance. In these cases, the user himself is responsible for compliance with the EMC limits.

Atlantis Land

Declaration of Conformity CE

Hereby, Sidin SpA, declares that this product (A02-RA111U) is in compliance to all relevant essential requirements of R&TTE Directive (99/5/CE). CE Declaration is available on the web site www.atlantis-land.com.

Important information for the correct recycle/treatment procedures of this equipment

The mentioned information are reported herewith in compliance with directive 2002/95/CE, 2002/96/CE and 2003/108/CE which requires a separate collection system and specific treatment and disposal procedures for the waste of electric and electronic equipments.

The crossed-out wheeled bin symbol printed on the unit label or unit packaging indicates that this equipment must not be disposed of as unsorted municipal waste but it should be collected separately.

The waste of electric and electronic equipment must be treated separately, in order to ensure that hazardous materials contained inside the equipment are not buried thereby providing potential future problems for the environment and human health.

Moreover, it will be possible to reuse and recycle some parts of the waste of electric and electronic equipment, contributing to reduce the quantities of waste to be disposed of and the depletion of natural resources.

As user of this equipment, you are responsible to contact the producer to know the correct procedure in the separate collection system for the waste of electric and electronic equipments.

Your rôle in participating to the separate collection of waste of electric and electronic equipment is essential to ensure that environmental protection and human health objectives connected to a responsible treatment and recycling activities are achieved.

1. Introduction

1.1 An Overview of WebShare 111U

Welcome to the WebShare 111U. Your WebShare 111U is an "all-in-one" unit, combining an ADSL2+ modem, ADSL router and Ethernet network switch, providing everything you need to get the machines on your network connected to the Internet over your ADSL broadband connection.

The WebShare 111U complies with ADSL2+ standards for worldwide deployment and supports downstream rates of up to 24 Mbps and upstream rates of up to 1 Mbps. It is designed for small office, home office and residential users, enabling even faster speed Internet connections. User can enjoy ADSL services and broadband multimedia applications such as interactive gaming, video streaming and real-time audio much easier and faster than ever before.

The product supports PPPoA (RFC 2364 – PPP (Point-to-Point Protocol) over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM (bridged or routed), PPP over Ethernet (RFC 2516), and IPoA (RFC1577) to establish a connection with ISP. The product also supports VC-based and LLC-based multiplexing.

It is the perfect solution to connect a small group of PCs to a high-speed broadband Internet connection. Multi-users can have high-speed Internet access simultaneously.

This product also serves as an Internet firewall, protecting your network from being accessed by outside users. Not only provide the natural firewall function (Network Address Translation, NAT), it also provides rich firewall features to secure user's network. All incoming data packets are monitored and filtered. Besides, it can also be configured to block internal users from accessing to the Internet.

The product provides two levels of security support. First, it masks LAN users' IP addresses which are invisible to outside users on the Internet, making it much more difficult for a hacker to target a machine on your network. Secondly, it can block and redirect certain ports to limit the services that outside users can access. For example, to ensure that games and other Internet applications will run properly, user can open some specific ports for outside users to access internal services in network.

Integrated DHCP (Dynamic Host Control Protocol) services, client and server, allow multiple users to get their IP addresses automatically on boot up from the product. Simply set local machines as a DHCP client to accept a dynamically assigned IP address from DHCP server and reboot. Each time local machine is powered up; the router will recognize it and assign an IP address to instantly connect it to the LAN.

For advanced users, Virtual Service function allows the product to provide limited visibility to local machines with specific services for outside users. An ISP (Internet Service Providers) provided IP address can be set to the product and then specific services can be rerouted to specific computers on the local network. For instance, a dedicated web server can be connected to the Internet via the product and then incoming requests for HTML that are received by the product can be rerouted to the dedicated local web server, even though the server now has a different IP address. In this example, the product is on the Internet and vulnerable to attacks, but the server is protected.

Virtual Server can also be used to re-task services to multiple servers. For instance, the product can be set to allow separated FTP, Web, and Multiplayer game servers to share the same Internet-visible IP address while still protecting the servers and LAN users from hackers.

1.2 Package Contents

Unpack the package and check all the items carefully. If any item contained is damaged or missing, please contact your local dealer as soon as possible. Also, keep the box and packing materials in case you need to ship the unit in the future. The package should contain the following items:

- 1 x WebShare 111U
- 1 x Power Supply
- 1 x Cat 5 LAN cable (RJ-45 connector)
- 1 x Phone cable (RJ-11 connector)
- 1 x USB cable
- 1 x Multilanguage Quick Start Guide (English, Italian and Francais)
- 1 x Cd-Rom with driver, utility and multilanguage manual
- 1 x Warranty Card
- 1 x WEEE Disclaimer

If any item is found missing or damaged, please contact your local reseller for replacement.

Atlantis Land

1.3 Technical Features

Technical charateristics of WebShare 111U:

- **ADSL Multi-Mode Standard:** supports downstream rates of up to 24 Mbps and upstream rates of up to 1 Mbps. It also supports rate management that allows ADSL subscribers to select an Internet access speed suiting their needs and budgets. It is compliant with Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt(G.992.1); G.lite(G992.2)), G.hs (G994.1), G.dmt.bis (G.992.3), G.dmt.bisplus (G.992.5)). The Annex A and B are supported in different H/W platforms.
- **Multi-Protocol to Establish A Connection:** Supports PPPoA (RFC 2364 - PPP over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM (bridged or routed), PPP over Ethernet (RFC 2516) and IPoA (RFC1577) to establish a connection with the ISP. The product also supports VC-based and LLC-based multiplexing.
- **Dual-Port Modem/Router:** A 10/100Mbps fast Ethernet router is built in with automatic switching between MDI and MDI-X for 10Base-T and 100Base-TX ports. An Ethernet straight or cross-over cable can be used directly for auto detection.
- **Network Address Translation (NAT):** Allows multi-users to access outside resources such as the Internet simultaneously with one IP address/one Internet access account. Many application layer gateway (ALG) are supported such as web browser, ICQ, FTP, Telnet, E-mail, News, Net2phone, Ping, NetMeeting, IP phone and others.
- **Firewall:** Supports simple firewall with NAT technology and provides option for blocking access from Internet, like Telnet, FTP, TFTP, WEB, SNMP and IGMP.
- **Domain Name System (DNS) relay:** Provides an easy way to map the domain name (a friendly name for users such as www.yahoo.com) and IP address. When a local machine sets its DNS server with this router's IP address, every DNS conversion request packet from the PC to this router will be forwarded to the real DNS in the outside network.
- **PPP over Ethernet (PPPoE):** Provides embedded PPPoE client function to establish a connection. Users can get greater access speed without changing the operation concept, sharing the same ISP account and paying

9

for one access account. No PPPoE client software is required for local computer. The Automatic Reconnect and Disconnect Timeout (Idle Timer) functions are provided, too.

- **Dynamic Host Control Protocol (DHCP) client and server:** In the WAN site, the DHCP client can get an IP address from the Internet Service Provider (ISP) automatically. In the LAN site, the DHCP server can allocate a range of client IP addresses and distribute them including IP address, subnet mask as well as DNS IP address to local computers. It provides an easy way to manage the local IP network.
- **RIP1/2 Routing:** Supports RIP1/2 routing protocol for routing capability.
- **Web based GUI:** Supports web based GUI for configuration and management. It is user-friendly and comes with on-line help. It also supports remote management capability for remote users to configure and manage this product.
- **Quick Installation Wizard:** Supports a WEB GUI page to install this device quickly. With this wizard, end users can   enter the information easily which they get from their ISP, then surf the Internet immediately.
- **Packet Filtering:** Up to 72 rules.
- **Universal Plug and Play (UPnP) e UPnP NAT Traversal:** This protocol is used to enable simple and robust connectivity among stand-alone devices   and PCs from many different vendors. It makes network simple and affordable for users. UPnP architecture leverages TCP/IP and the Web to enable seamless proximity networking in addition to control and data transfer among networked devices. With this feature enabled, users can now connect to Net meeting or MSN Messenger seamlessly.
- **Virtual Server:** User can specify some services to be visible from outside users. The router can detect incoming service request and forward it to the specific local computer to handle it. For example, user can assign a PC in LAN acting as WEB server inside and expose it to the outside network. Outside user can browse inside web server directly while it is protected by NAT. A DMZ host setting is also provided to a local computer exposed to the outside network, Internet.

1.4 WebShare 111U Application

Follow the followings steps to cabling the device:

- Connect WAN Port to the telephone line throught RJ-11 cable (contained in package).
- WebShare 111U can be connect in the following configuration:
  - ➢ Directly to the PC, throught CAT5 cables (one is contained in package) or USB cable (also provided with the device).
  - ➢ To an Hub/Switch throught UPLINK Port thought CAT 5 cable (contained in package).
- Connect AC-DC Adapter on AC and on device (POWER jack) in the reat r of the product.
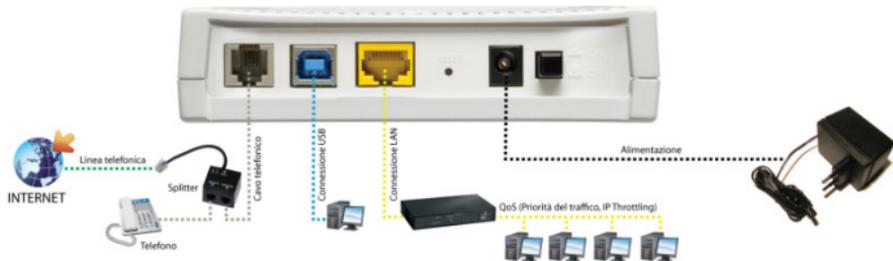
2. Using WebShare 111U

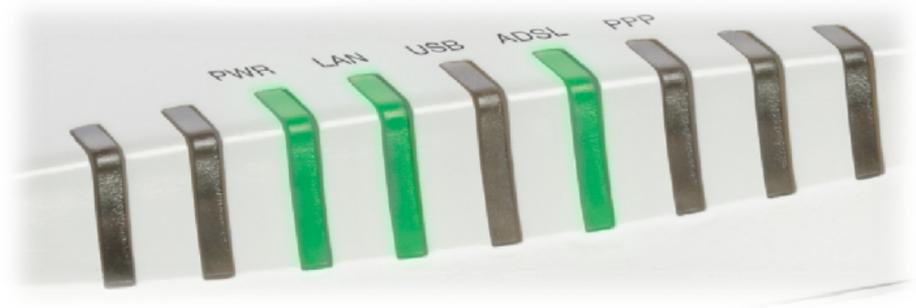## 2.1 Cautions for using the WebShare 111U

- Do not place the 111U under high humidity and high temperature.
- Do not use the same power source for 111U with other equipment.
- Do not open or repair the case yourself.
- If the 111U is too hot, turn off the power immediately and have a qualified serviceman repair it.
- Place the 111U on a stable surface.
- Only use the power adapter that comes with the package.

2.2 The Front LEDs

LED	MEANING
PWR	Lit red when power is ON. Lit green when the system is ready.
LAN	• Lit when connected to an Ethernet device. • Lit green for both 10M and 100M. • Blinking when data is Transmitted / Received.
USB	Lit when the device is connected to the PC and is working properly.
ADSL	Lit when successfully connected to an ADSL DSLAM ("linesync").
PPP	• Lit red when WAN fails to get IP address. • Lit green when WAN gets the IP address.

2.3 The Rear Ports

PORT	MEANING
LINE (RJ11)	Connect the supplied RJ-11 ("telephone") cable to this port when connecting to the ADSL/telephone network.
USB	User can connect to PC using an alternative USB cable through this port.
LAN (RJ45)	Connect a UTP Ethernet cable (Cat-5 or Cat-5e) to the Ethernet port when connecting to a PC or an office/home network of 10Mbps or 100Mbps.
RESET	After the device is powered on, press it to reset the device or restore to factory default settings. • **0-3 seconds:** reset the device • **6 seconds above:** restore to factory default settings (this is used when you cannot login to the router, e.g. forgot the password)
POWER (jack)	Connect the supplied power adapter to this jack.
POWER (On/Off)	Power ON/OFF switch.

2.4 Cabling

First you must connect the product to the ADSL line through the RJ11 cable you have in equipment (in the port **LINE**) and connect the AC Adapter to the WebShare 111U and then to the socket. Once you've checked all the connections and you've switched on the Router the product will carry on immediately a diagnosis (about 10 seconds). Finished this, the Led **PWR** will be fixed green and Led **PPP** will be fixed red; DSL will blink during sinchonization, and will be fixed when ADSL line is synchronized with WebShare 111U. If Led DSL blink continuously, please contact Your ISP in order to check ADSL line state.

Ensure that all other devices connected to the same telephone line as your WebShare (e.g. telephones, fax machines, analog modems) have a line filter (**A01-AF2**) connected between them and the wall socket (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and ensure that all line filters are correctly installed and the right way around.

2.5 Ethernet Connection

WebShare 111U is equipped with a 10/100 Mbps Ethernet port (with RJ-45 connector) to permits the connection between a PC (with Fast Ethernet NIC and TCP/IP stack installed) and the Modem/Router.

NOTE:

For operationg systems older than Windows 2000, you might install TCP/IP stack separately in order to use WebShare 111U.

After cable connection, WebShare 111U will provide automatically an IP Address to the PC connected (the DHCP range is 192.168.1.100-192.168.1.199).

NOTE:

For any problem with DHCP Server service, please refer to "TCP/IP Configuration".

Atlantis Land
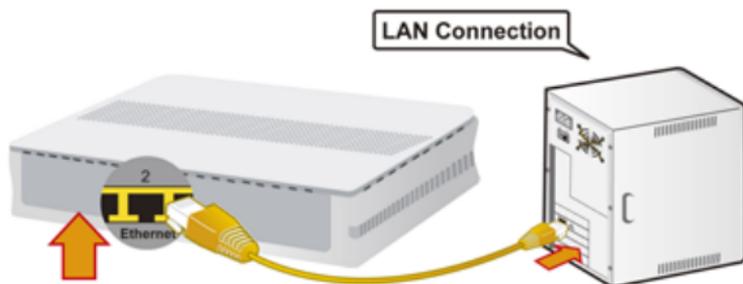
2.6 USB Connection

NOTE: **Do not plug USB Modem to Your PC before install USB driver.**

WebShare 111U also has provided with an USB port in order to connect the device with a PC using a free USB port (rev1.1 or 2.0).

2.7 USB Driver

To use WebShare 111U with USB connection, You have to install driver provided into Cd-Rom. Please follow this instructions in order to install USB driver:

1. Insert the CD-ROM and the Auto-run program will appear. Altenatively, you may need to proceed the software manually; go to your Windows Start menu and choose Run, type "**<CDROM>:\A02-RA111U\Driver\<OSVer>\SETUP.EXE**" in dialog box and click OK.
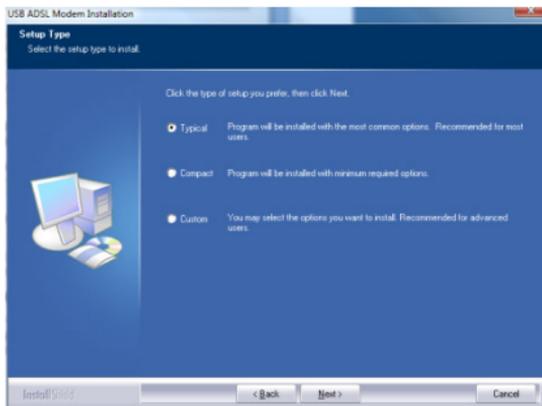
NOTE: D:\ will depends on where the CD-ROM drive is located and <Windows OS> will depend on the Windows OS you are using.

2. Click on "**A02-RA111U**" icon to select WebShare 111U Home Page.
3. Select the driver according to your operating system, and the install wizard will begin installing the software.
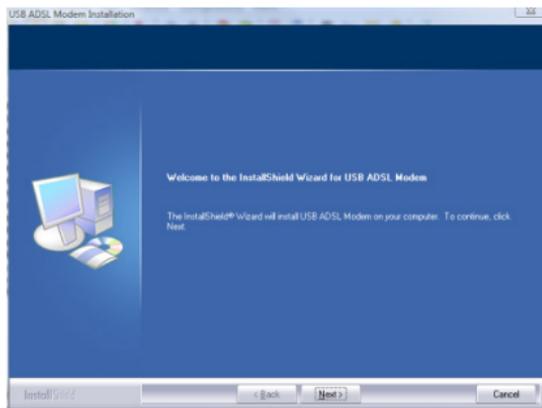
4. Select the installation mode between **Typical** (suggested), **Compact** and **Custom**.

4a. Choosing **Custom** installation's method, you have to confirm destination path for driver installation and which components You have to install.

5. Now, the installation utility will ask You to plug USB modem to your PC.

Atlantis Land

NOTE: When You plug USB modem to your PC, the operating system can start an automatic procedure to install new devices; please stop this in order to complete the installation.

6. Follow instructions shown on the screen in order to complete the installation.

3. Installing WebShare 111U

Before configuring this device, you have to check with your ISP (Internet Service Provider) what kind of service is provided such as PPPoE, PPPoA, RFC1483, or IPoA. Gather the information as illustrated in the following table and keep it for reference.

PPPoE	VPI and VCI VC-based / LLC-based multiplexing Username and Password Service Name
PPPoA	VPI and VCI VC-based / LLC-based multiplexing Username and Password
RFC1483 Bridged	VPI/VCI VC-based / LLC-based multiplexing
RFC1483 Routed	VPI/VCI VC-based / LLC-based multiplexing IP address Subnet mask Default Gateway (IP address) IP address (DNS)

3.1 Factory Default Setting

Before configuring your, you need to know the following default settings:

![Atlantis Land logo]

- Username: **admin**
- Password: **atlantis**
- LAN IP Address: **192.168.1.254**
- Subnet Mask: **255.255.255.0**
- ISP setting in WAN side: **PPPoA, VCMux, Routing, VPI=8, VCI=35**
- Firewall=**Enabled** , SPI=**Disabled**
- **DHCP Server enabled** with IP pool from 192.168.1.100 to 192.168.1.199

> ⚠ If you ever forget the password to log in, you may press the RESET button up to 6 seconds to restore the factory default settings.

LAN Interface		WAN Interface
IP address	192.168.1.254	Mode=**Routing**
Subnet Mask	255.255.255.0	Encapsulation=**PPPoA**
DHCP Server	Enabled	Multiplex=**VC**
DHCP Server IP Pool	100 IP available (from 192.168.1.100 to 192.168.1.199)	VPI=**8** VCI=**35**

3.2 TCP/IP Configuration

PCs must have an Ethernet interface installed properly and be connected to the router either directly or through an external repeater hub, and have TCP/IP installed and configured to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. The default IP address of the router is 192.168.1.254 and the subnet mask is 255.255.255.0 (i.e. any attached PC must be in the same subnet, and have an IP address in the range of 192.168.1.1 to 192.168.1.253). The best and easiest way is to configure the PC to get an IP address automatically from the router using DHCP. If you encounter any problems accessing the router's web interface it may also be advisable to uninstall any kind of software firewall on your PCs, as they can cause problems accessing the 192.168.1.254 IP address of the router. Users should make their own decisions on how to best protect their network.

Atlantis Land

Please follow the steps below for your PC's network environment installation. First of all, please check your PC's network components. The TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to your Windows-related or other operating system manuals.

NOTE: Any TCP/IP capable workstation can be used to communicate with or through the WebShare 111U. To configure other types of workstations, please consult the manufacturer's documentation.

Configuring PC (Windows 2000)

1. Go to **Start** -> **Settings** -> **Control Panel**. In the Control Panel, double-click on **Network and Dial-up Connection**s.
2. Double-click **LAN Area Connection**.
3. In the LAN Area Connection Status window, click **Properties**.
4. Select **Internet Protocol (TCP/IP)** and click **Properties**.
5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.
6. Click **OK** to finish the configuration.

Configuring PC (Windows XP)

1. Go to **Start** -> **Control Panel** (in Classic View). In the Control Panel, double-click on **Network Connections**.
2. Double-click **Local Area Connection**.
3. In the LAN Area Connection Status window, click **Properties**.
4. Select **Internet Protocol (TCP/IP)** and click **Properties**.
5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.
6. Click **OK** to finish the configuration

Configuring PC (Windows Vista)

1. Go to **Start** -> **Control Panel** (in Classic View). In the Control Panel, double-click on **Network and Sharing Center** icon.
2. Click **Manage Network connections** then double-click Local Area Connection. Click **Properties**.
3. Click **Continue** (Windows needs your permission to continue).
4. Select **Internet Protocol Version 4 (TCP/IP)** and click **Properties**.
5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.
6. Click **OK** to finish the configuration.

Configuring for MAC

7. Click on **Apple** Menu and select **Control Panel/TCP/IP**. It will appear the follow screen.
8. Select **Ethernet** on **Connect Via**.
9. Select **Using DHCP Server** on Configure.
10. Leave empty the field **DHCP Client ID**.

3.3 Verification of TCP/IP Configuration

To verify your correct configuration (after PC restart, necessary for Windows 98, 98Se, ME and instead enough obtain IP lease for XP, 2000),use ping command. From a DOS Window, type:

ping 192.168.1.254

If It show you this message:

> **Pinging 192.168.1.254 with 32 bytes of data:**
> **Reply from 192.168.1.254: bytes=32 times<10ms TTL=64**
> **Reply from 192.168.1.254: bytes=32 times<10ms TTL=64**
> **Reply from 192.168.1.254: bytes=32 times<10ms TTL=64**

It i s possibile to continue to follow step. If it show you follow message:

> **Pinging 192.168.1.254 with 32 bytes of data:**
> **Request timed out.**
> **Request timed out.**
> **Request timed out.**

Check that LAN LED is lit (change CAT cable if is not). Check PC IP Address typing **winipcfg** for (Win95,98,ME) or **ipconfig** (for Win2000,XP) and eventually re-install TCP/IP stack.

3.4 Browser Configuration

Now open IE, go to **Instruments** menu, select the **Connections** tab and select one of the following options:

- Never use remote connection
- Use remote connection if another network connection isn't available

4. Configuration with utility

4.1 WebShare Configuration Utility

WebShare 111U has provided with an easy installation utility in order to make installation more easy and simple.
To start the configuration utility, please follow these instructions:

1. Insert the CD-ROM and the Auto-run program will appear. Altenatively, you may need to proceed the software manually; go to your Windows Start menu and choose Run, type "**<CDROM>:\A02-RA111U\Utility\UTILITY.EXE**" in dialog box and click OK.

NOTE:

D:\ will depends on where the CD-ROM drive is located and <Windows OS> will depend on the Windows OS you are using.

2. Click on **WebShare Configuration Assistant** icon to select the utility.

Step 1: Welcome
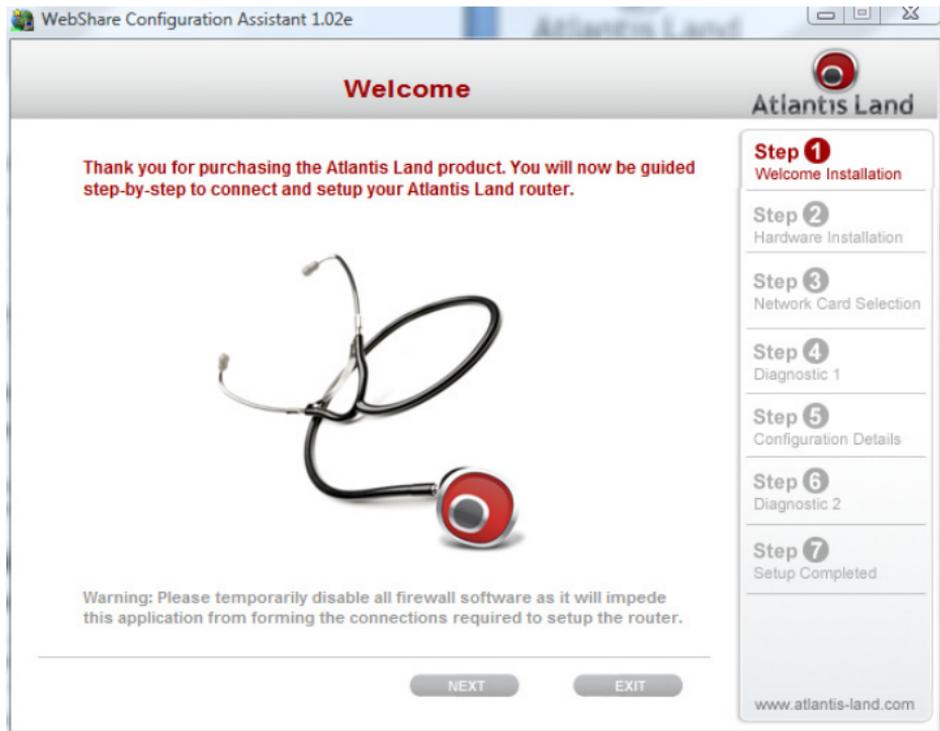
Step 2: Hardware Installation

The Hardware Installation screen will appear. Four links are shown on the screen. Click them one by one and follow the guidelines to complete hardware installation.

Atlantis Land

**Step 3: Network Card Selection**

NOTE: Please select **ADSL Company ADSL USB Modem** interface to use WebShare thorough USB port. If this interface will not show into the interface list, please remove and re-install USB driver.
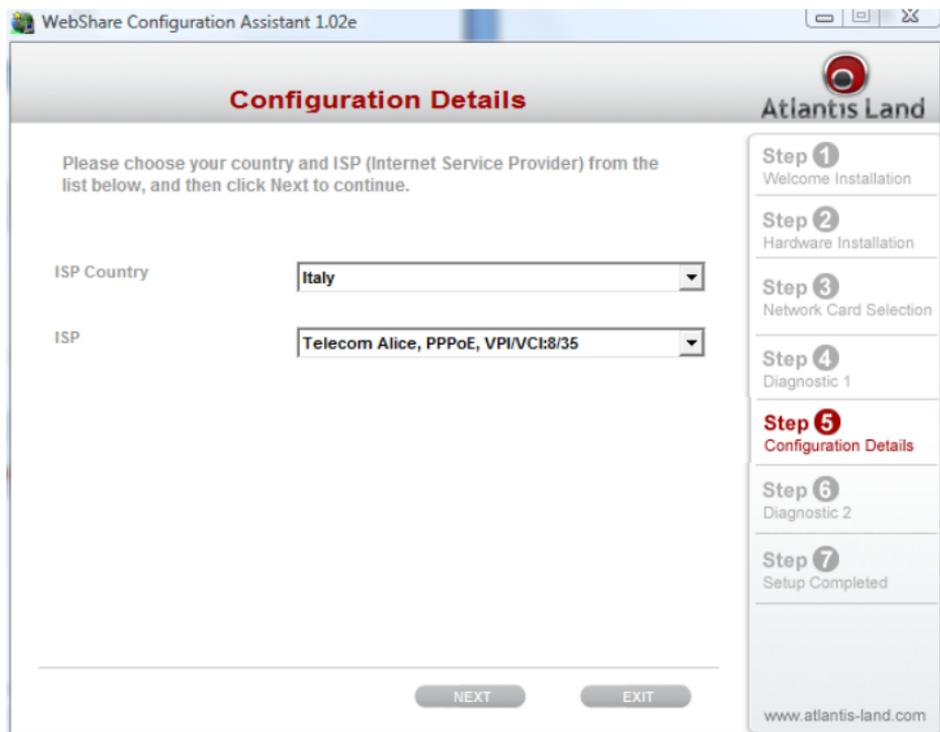

WebShare Configuration Assistant 1.02e

Network Card Selection

Atlantis Land

192.168.1.100 Intel(R) 82566MC Gigabit Network Connection

Please select the network card which is connected to the router.

INDIETRO   NEXT   EXIT

Step 1
Welcome Installation

Step 2
Hardware Installation

Step 3
Network Card Selection

Step 4
Diagnostic 1

Step 5
Configuration Details

Step 6
Diagnostic 2

Step 7
Setup Completed

www.atlantis-land.com

![Atlantis Land logo]

Step 4: Diagnostic 1

If connection fails, the screen will show **FAIL**, please check your router if it is connected correctly.
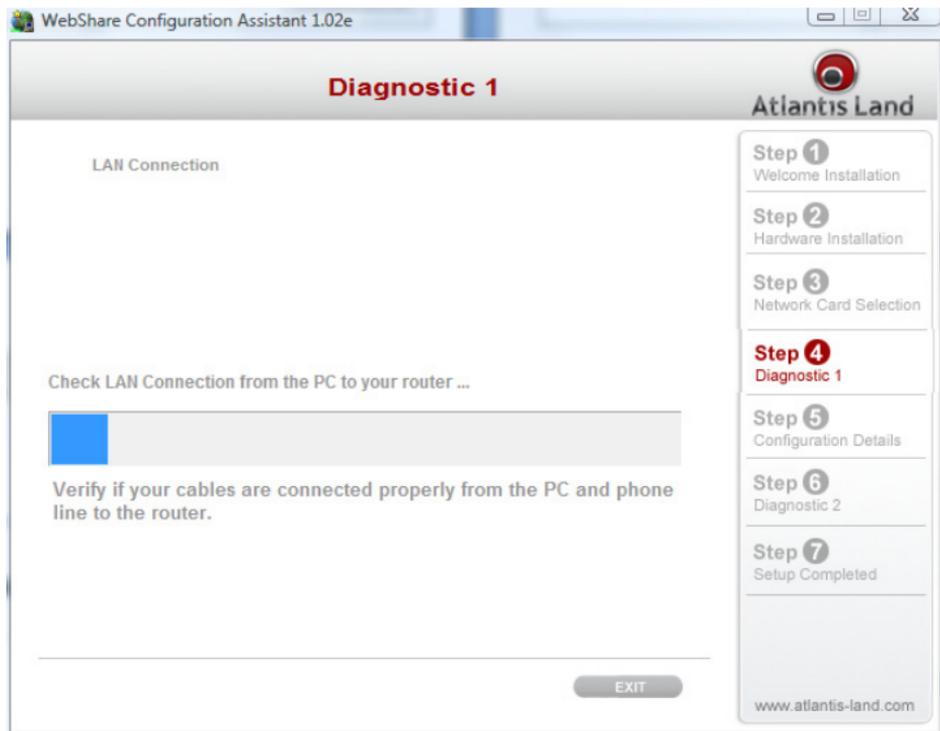
Step 5: Configuration Details

Set up more detailed settings such as VPI, VCI and MTU.

Please enter **Username** and **Password** as supplied by your ISP (Internet Service Provider).

Step 6: Diagnostic 2
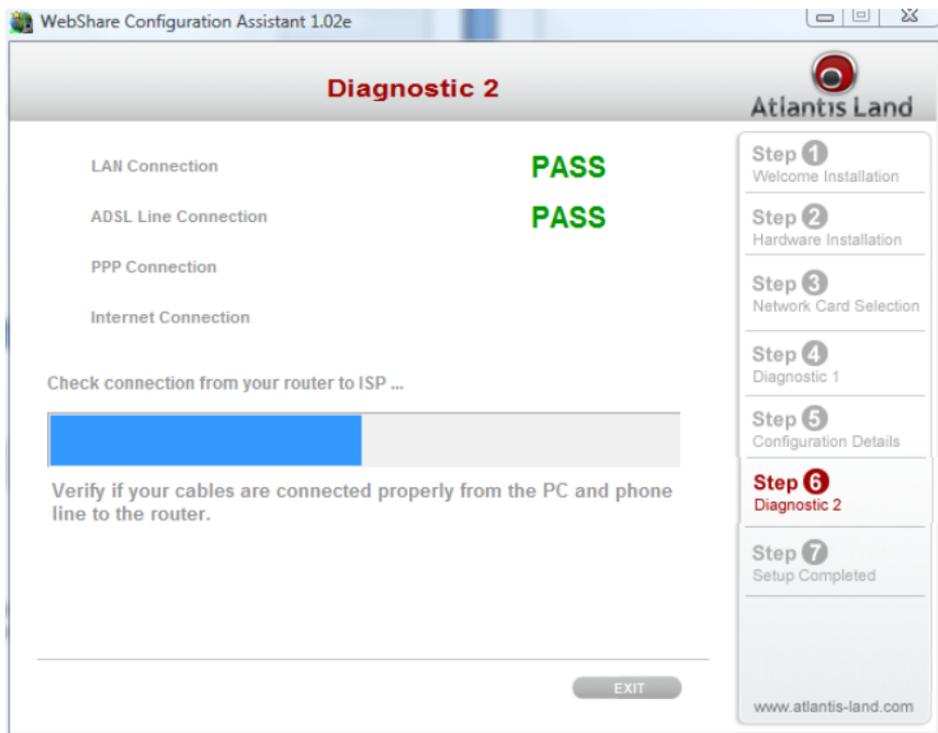
Diagnostic 2

Atlantis Land

LAN Connection	**PASS**
ADSL Line Connection	**PASS**
PPP Connection	
Internet Connection	

Check connection from your router to ISP ...

Verify if your cables are connected properly from the PC and phone line to the router.

Step 1 Welcome Installation

Step 2 Hardware Installation

Step 3 Network Card Selection

Step 4 Diagnostic 1

Step 5 Configuration Details

Step 6 Diagnostic 2

Step 7 Setup Completed

EXIT

www.atlantis-land.com

Step 7: Setup Completed

Congratulations!! You've completed the setup procedure and are ready to surf the Internet. The IE browser will open up automatically when you finish installing.
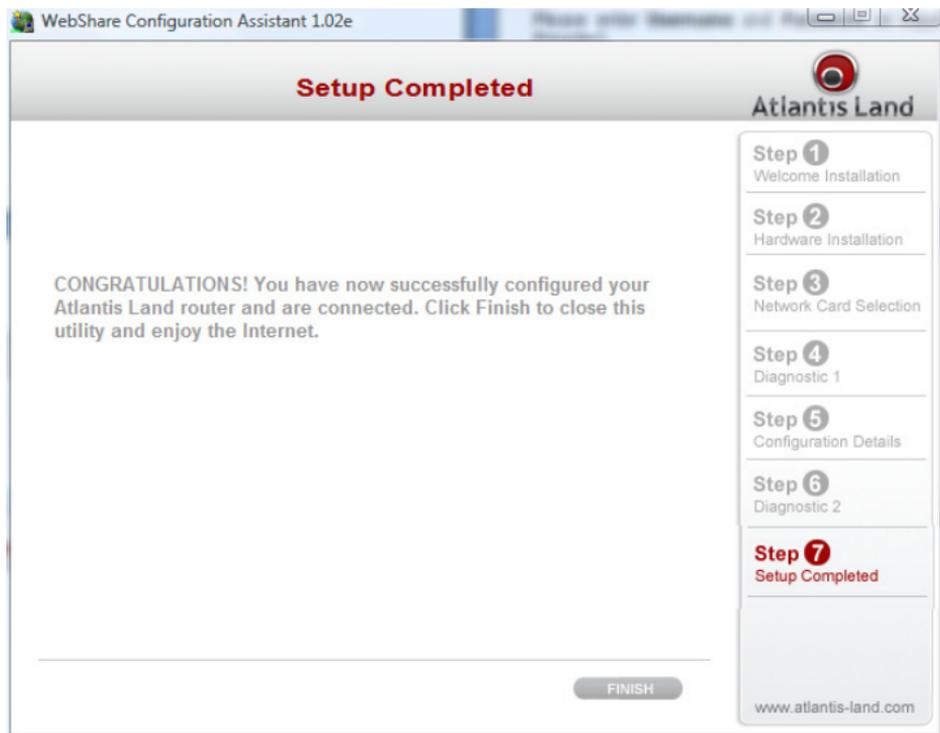
4.2 Browser Configuration

Open your web browser, enter the IP address of your router, which by default is 192.168.1.254, and click **Go**.

The default username and password are **admin** and **atlantis**.

Now, You have access to the Site Map Configuration Interface, subdivided as following:

- **Quick Start** (Run Wizard)
- **Interface Setup** (Internet, LAN)
- **Advanced Setup** (Routing, NAT, QoS, ADSL, Firewall)
- **Access Management** (ACL, IP Filter, SNMP, UPnP, DDNS)
- **Maintenance** (Administration, Time Zone, Firmware, SysRestart, Diagnostics)
- **Status** (Device Info, System Log, Statistics)

Click on the desired item to expand the page with all settings in the main navigation panel.

4.3 Configuring Password

It is highly recommended that you change the password for accessing the ADSL Router. To change the ADSL Router' password, click **Maintenance** and then **Administration** . The screen appears as shown:
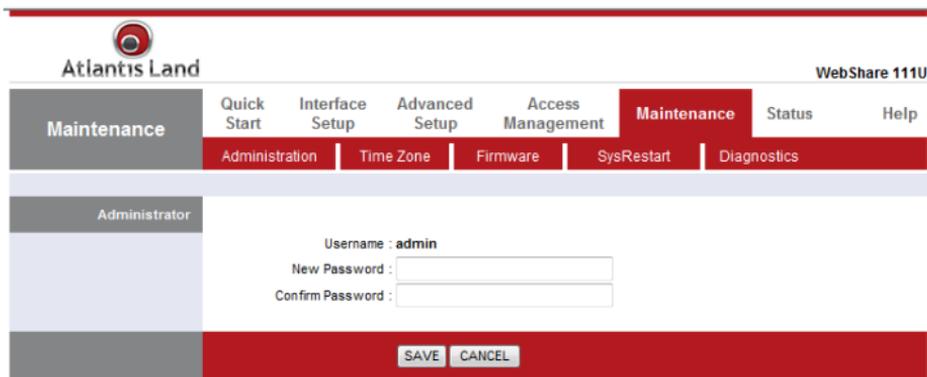
The following table describes the labels in this screen:

Label	Description
New Password	Type the new password in this field.
Confirm Password	Type the new password again in this field.
Save	Click Apply to save your changes back to the ADSL Router.
Cancel	Click Cancel to begin configuring this screen afresh.

4.4 Resetting the WebShare 111U

If you forget your password or cannot access the WebShare 111U, you will need to reload the factory-default configuration file or use the **RESET** button the back of the ADSL Router. Uploading this configuration file replaces the current configuration file with the factory-default configuration file.

4.4.1 Using the RESET button

1.   Make sure the SYS PWR is on (not blinking).

2. Press the RESET button for 10 (or more) seconds, and then release it. When the PWR LED begins red, the defaults have been restored and the ADSL Router restarts.

5. Quick Start

This chapter provides information on the Wizard Setup screens in the web configurator.

5.1 Wizard Setup Introduction

Use the Wizard Setup screens to configure your system for Internet access settings and fill in the fields with the information in the Internet Account Information table of the Compact Guide or Read Me First. Your ISP may have already configured some of the fields in the wizard screens for you.

5.1.1 Encapsulation

Be sure to use the encapsulation method required by your ISP. The ADSL Router supports the following methods:

- **PPP over Ethernet (PPPoE RFC 2516):** PPPoE provides access control and billing functionality in a manner similar to dial-up services using PPP. The ADSL Router bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your computer to an ATM PVC (Permanent Virtual Circuit) which connects to ADSL Access Concentrator where the PPP session terminates. One PVC can support any number of PPP sessions from your LAN. For more information on PPPoE, see the appendix.
- **PPP over ATM (PPPoA RFC2364):** PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). It provides access control and billing functionality in a manner similar to dial-up services using PPP. The ADSL Router encapsulates the PPP session based on RFC1483 and sends it through an ATM PVC (Permanent Virtual Circuit) to the Internet Service Provider's (ISP) DSLAM (digital access multiplexer). Please refer to RFC 2364 for more information on PPPoA. Refer to RFC 1661 for more information on PPP.

- **RFC 1483 (Bridged and Routed Mode):** RFC 1483 describes two methods for Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5). The first method allows multiplexing of multiple protocols over a single ATM virtual circuit (LLC-based multiplexing) and the second method assumes that each protocol is carried over a separate ATM virtual circuit (VC-based multiplexing). Please refer to the RFC for more detailed information.

5.1.2 Multiplexing

There are two conventions to identify what protocols the virtual circuit (VC) is carrying. Be sure to use the multiplexing method required by your ISP.
The WebShare 111U Modem/Router supports followings tran sport methods:

- **VC-Based Multiplexing:** In this case, by prior mutual agreement, each protocol is assigned to a specific virtual circuit; for example, VC1 carries IP, etc. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.
- **LLC-Based Multiplexing:** In this case one VC carries multiple protocols with protocol identifying information being contained in each packet header. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol, for example, if charging heavily depends on the number of simultaneous VCs.

5.1.3 VPI and VCI

Be sure to use the correct Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) numbers assigned to you. The valid range for the VPI is 0 to 255 and for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Please see the appendix for more information.

5.1.4 Quick Start

Following next steps you can make operating WebShare 111U in short time using PCs in DHCP mode. Click on **Quick Start** then Run Wizard to perform an automatic protocol selection.

The following screen will appear:

You can change the password as you like and then click **Next** to continue; select your time zone from the drop down list. Please click **Next** to continue.

Select how the router will set up the Internet connection:

- **PPPoE/PPPoA:** to obtain IP automatically (You need username and password).
- **Static IP address:** this configuration is valid in case of a subscription with a static IP.

PPPoE/PPPoA

PPPoE (PPP over Ethernet) is an ADSL connection known as dial-up DSL. As the PPPoA it has been created to integrate large band services paying a particular attention to an easy configuration. The user can obtain an high access speed and he can also share the same account with the ISP. No additional software are required. This configuration is valid in case of a subscription with a static IP and active NAT (SUA) (for the managing of the public class turn to the CD handbook). Let's see how to configure correctly this kind of ADSL configuration.

Insert **Username** and **Password** and make sure that the parameters are, in case of PPPoA, the ones in the picture, if not specifically shown by the ISP.

In case of **PPPoE** choose **Connection Type=PPPoE LLC** and click on **Next**.

NOTE: You have to pay particular attention to the WAN-ADSL connection. If you have any doubt turn to qualified personnel or contact Atlantis-Land technical assistance. Atlantis Land will not be considered responsible in case of wrong or bad configuration.

Static IP Address

This configuration is valid in case of a subscription with a static IP and active NAT SUA (for the managing of the public class turn to the CD Manual). Make sure that the parameters are, in case of **RFC1483**, the ones in the picture, if not specifically shown by the ISP.

Insert then the public static IP address given by the ISP and choose **Connection Type=1483 Routed IP LLC(IPoA)**. Make sure that the parameters are, the ones in the picture, if not specifically shown by the ISP.

Cliccare on **Next**.

5.1.5 Wizard Setup Configuration: Connection Tests

Launch your web browser and navigate to www.atlantis-land.com Internet access is just the beginning. Refer to the rest of this User's Guide for more detailed information on the complete range of ADSL Router features. If you cannot access the Internet, open the web configurator again to confirm that the Internet settings you configured in the Wizard Setup are correct.

The Webshare 111U automatically tests the connection to the computer(s) connected to the LAN ports. To test the connection from the ADSL Router to the ISP, click **Maintenance** then **Diagnose**.

6. LAN Setup

This chapter describes how to configure LAN settings.

6.1 LAN Overview

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building.
The LAN screens can help you configure a LAN DHCP server and manage IP addresses.

6.1.1 LANs, WANs and the ADSL Router

The actual physical connection determines whether the ADSL Router ports are LAN or WAN ports. There are two separate IP networks, one inside, the LAN network; the other outside: the WAN network as shown next:
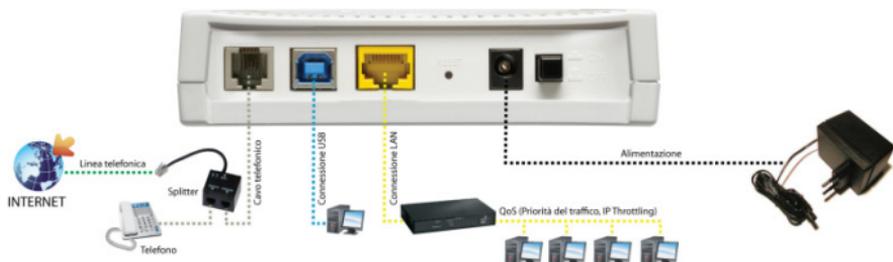
6.2 DNS Server Address

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa, for example, the IP address of www.atlantis-land.com is 204.217.0.2. The DNS server is extremely important because without it, you must

know the IP address of a machine before you can access it. The DNS server addresses that you enter in the DHCP setup are passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses. The first is for an ISP to tell a customer the DNS server addresses, usually in the form of an information sheet, when s/he signs up. If your ISP gives you the DNS server addresses, enter them in the DNS Server fields in DHCP Setup, otherwise, leave them blank.

Some ISP's choose to pass the DNS servers using the DNS server extensions of PPP IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The ADSL Router supports the IPCP DNS server extensions through the DNS proxy feature.

If the Primary and Secondary DNS Server fields in DHCP Setup are not specified, for instance, left as 0.0.0.0, the ADSL Router tells the DHCP clients that it itself is the DNS server. When a computer sends a DNS query to the ADSL Router, the ADSL Router forwards the query to the real DNS server learned through IPCP and relays the response back to the computer.

Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make sure that you enter their IP addresses in the DHCP Setup menu. This way, the ADSL Router can pass the DNS servers to the computers and the computers can query the DNS server directly without the ADSL Router's intervention.

6.3 DNS Server Address Assignment

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

There are two ways that an ISP disseminates the DNS server addresses:

1. The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the DNS Server fields in DHCP Setup.

2. Leave the DNS Server fields in DHCP Setup blank (for example 0.0.0.0). The ADSL Router acts as a DNS proxy when this field is blank.

6.4 LAN TCP/IP

The ADSL Router has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

6.4.1 Factory LAN Defaults

The LAN parameters of the ADSL Router are preset in the factory with the following values:

1. IP address of 192.168.1.254 with subnet mask of 255.255.255.0 (24 bits)
2. DHCP server enabled with 100 client IP addresses starting from 192.168.1.100.

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), read the embedded web configurator help regarding what fields need to be configured.

6.4.2 IP Address and Subnet Mask

Refer to the **IP Address** and **Subnet Mask** section in the Wizard Setup chapter for this information.

6.4.3 RIP Setup

RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The RIP Direction field controls the sending and receiving of RIP packets. When set to:

1. **Both** - the ADSL Router will broadcast its routing table periodically and incorporate the RIP information that it receives.
2. **In Only** - the ADSL Router will not send any RIP packets but will accept all RIP packets received.
3. **Out Only** - the ADSL Router will send out RIP packets but will not accept any RIP packets received.

4. **None** - the ADSL Router will not send any RIP packets and will ignore any RIP packets received.

The Dynamic Route field controls the format and the broadcasting method of the RIP packets that the ADSL Router sends (it recognizes both formats when receiving). RIP-1 is universally supported; but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology.
Both RIP-2B and RIP-2M sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting.
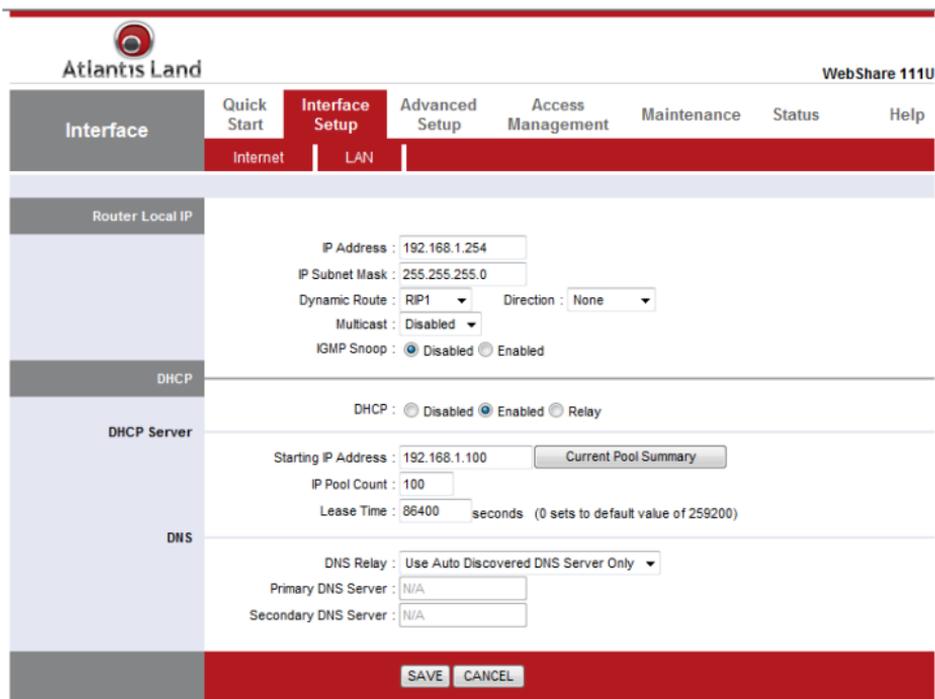
6.4.4 Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.
IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.
The ADSL Router supports both IGMP version 1 (IGMP-v1) and IGMP version 2 (IGMP-v2). At start up, the ADSL Router queries all directly connected networks to gather group membership. After that, the ADSL Router periodically updates this information. IP multicasting can be enabled/disabled on the ADSL Router LAN and/or WAN interfaces in the web configurator (LAN; WAN). Select None to disable IP multicasting on these interfaces.

6.5 Configuring LAN

Click **Interface Setup**, then **LAN** to open the following screen:

The following table describes the labels in this screen:

Router Local IP	
Field	**Description**
IP Address	Enter the IP address of the ADSL Router in dotted decimal notation, for example, 192.168.1.254 (factory default).
IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).

RIP Direction	Select the RIP direction from None, Both, In Only and Out Only.
Dynamic Route	Select the RIP version from RIP-1, RIP-2B and RIP-2M.
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a multicast group. The ADSL Router supports both IGMP version 1 (IGMP-v1) and IGMP-v2. Select None to disable it.
IGMP Snoop	Choose Disable or Enable IGMP Snoop function
Save	Click this button to save these settings back to the ADSL Router.
Cancel	Click this button to reset the fields in this screen.

DHCP

Field	Description
DHCP	If set to **Enabled**, the ADSL Router can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client. If set to **Disabled**, the DHCP server will be disabled. If set to **Relay**, the ADSL Router acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the Remote DHCP Server field in this case. When DHCP is used, the following items need to be set:
Starting IP Address	This field specifies the first of the contiguous addresses in the IP address pool.
IP Pool count	This field specifies the size or count of the IP address pool.
Lease Time	This field specifies the length of time for the IP lease.
DNS Relay	If user want to disable this feature, he just need to set both Primary and secondary DNS IP to 0.0.0.0. Using DNS relay, users can setup DNS server IP to 192.168.1.1 on their Computer. If not, device will perform as no DNS relay.
Primary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Secondary DNS Server	As above.
Save	Click this button to save these settings back to the ADSL Router.
Cancel	Click this button to reset the fields in this screen.

7. WAN Setup

This chapter describes how to configure WAN settings.

7.1 WAN Overview

A WAN (Wide Area Network) is an outside connection to another network or the Internet.
See the Wizard Setup chapter for more information on the fields in the WAN screens.

7.2 PPPoE Encapsulation

The ADSL Router supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The PPPoE option is for a dial-up connection using PPPoE.
For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example Radius). PPPoE provides a login and authentication method that the existing Microsoft Dial-Up Networking software can activate, and therefore requires no new learning or procedures for Windows users.
One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.
Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.
By implementing PPPoE directly on the ADSL Router (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the ADSL Router does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

7.3 PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.
PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet.

7.4 Traffic Shaping

Traffic Shaping is an agreement between the carrier and the subscriber to regulate the average rate and "burstiness" or fluctuation of data transmission over an ATM network. This agreement helps eliminate congestion, which is important for transmission of real time data such as audio and video connections.

Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum speed of 832 Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent on the line speed.

Sustained Cell Rate (SCR) is the mean cell rate of a bursty, on-off traffic source that can be sent at the peak rate, and a parameter for burst-type traffic. SCR may not be greater than the PCR; the system default is 0 cells/sec.

Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR. After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again.The following figure illustrates the relationship between PCR, SCR and MBS.
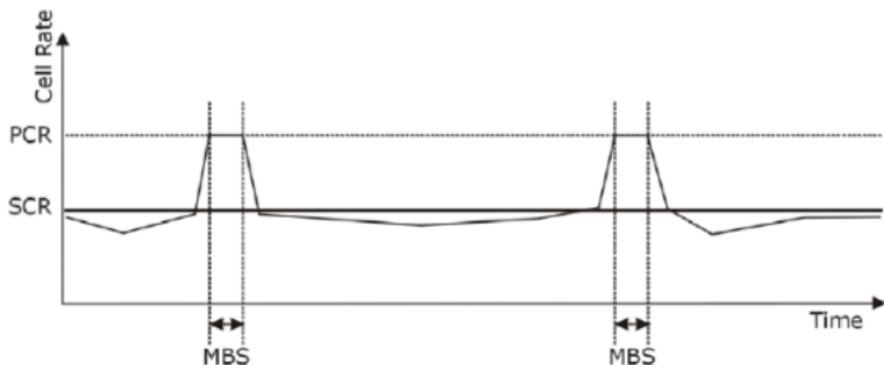
7.5 Configuring WAN Setup

To change the ADSL Router's WAN remote node settings, click **Interface Setup** then **Internet**. The screen differs by the encapsulation.

The following table describes the labels in this screen:

Field	Description
ATM VC	
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit.
Status	Activated or Deactivated
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you. This field may already be configured.
VCI	The valid range for the VCI is 32 to 65535. Enter the VCI assigned to you. This field may already be configured.
ATM QoS	Select CBR (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select UBR (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select VBR (Variable Bit Rate) for bursty traffic and bandwidth sharing with other applications. VBR is not available on all models.
Cell Rate	Cell rate configuration often helps eliminate traffic congestion that slows transmission of real time data such as audio and video connections.
Peak Cell Rate (PCR)	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.
Sustain Cell Rate (SCR)	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR.
Maximum Burst Size (MBS)	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.
ENCAPSULATION	
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box.
PPPoA/PPPoE	

Service Name	(PPPoE only) Type the name of your PPPoE service here.
User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. The Single User Account feature can be used with either a dynamic or static IP address. Select Obtain an IP Address Automatically if you have a dynamic IP address; otherwise select Static IP Address and type your ISP assigned IP address in the IP Address field below.
Multiplex	Select the method of multiplexing used by your ISP from the drop-down list. Choices are VC or LLC.

Connection Settings	
Always ON	Select Always ON Connection when you want your connection up all the time. The ADSL Router will try to bring up the connection automatically if it is disconnected.
Connect on Demand	Connect on demand is dependent on the traffic. If there is no traffic (or Idle for a pre-specified period of time), the connect will tear down automatically. And once there is traffic send or receive, the connection will be automatically on. Please insert the Idle Time in minute.

IP Address	
Get IP Address	The IP address can be either dynamically (via DHCP) or given IP address provide by your ISP. For Static IP, you need to specify the IP address, Subnet Mask and Gateway IP address.
IP Address	You must specify a Router IP address.
IP Subnet Mask	Enter a subnet mask in dotted decimal notation. Refer to the Subnetting appendix in the to calculate a subnet mask If you are implementing subnetting.
Gateway	You must specify a gateway IP address.
NAT	Select this option to Activate/Deactivated the NAT (Network

48

	Address Translation) function for this VC. The NAT function can be activated or deactivated per PVC basis.
Default Route	if enable this function, the current PVC will be the default gateway to internet from this device.
TCP MTU Option	RIP (Routing Information protocol) Select this option to specify the RIP version, including RIP-1, RIP-2M and RIP-2B. RIP-2M and RIP-2B are both sent in RIP-2 format; the difference is that RIP-2M using Multicast and RIP-2 using Broadcast format.
Dynamic Route	RIP Direction Select this option to specify the RIP direction. None is for disabling the RIP function. Both means the ADSL Router will periodically send routing information and accetp routing information then incorporate into routing table. IN only means the ADLS router will only accept but will not send RIP packet. OUT olny means the ADLS router will only send but will not accept RIP packet.
Direction	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a multicast group. The ADSL ATU-R supports both IGMP version 1 (IGMP-v1) and IGMP-v2. Select None to disable it.
Multicast	Click Apply to save the changes.
Save	The IP address can be either dynamically (via DHCP) or given IP address provide by your ISP. For Static IP, you need to specify the IP address, Subnet Mask and Gateway IP address.

8. Network Address Translation (NAT)

This chapter discusses how to configure NAT on the WebShare Wireless Router ADSL2+.

8.1 NAT Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

8.1.1 NAT Definitions

Inside/outside denotes where a host is located relative to the ADSL Router, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

| Item	Description
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

8.1.2 What NAT Does

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. With no servers defined, the ADSL Router filters out all incoming inquiries, thus

preventing intruders from probing your network. For more information on IP address translation, refer to RFC 1631, The IP Network Address Translator (NAT).

8.1.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The ADSL Router keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.
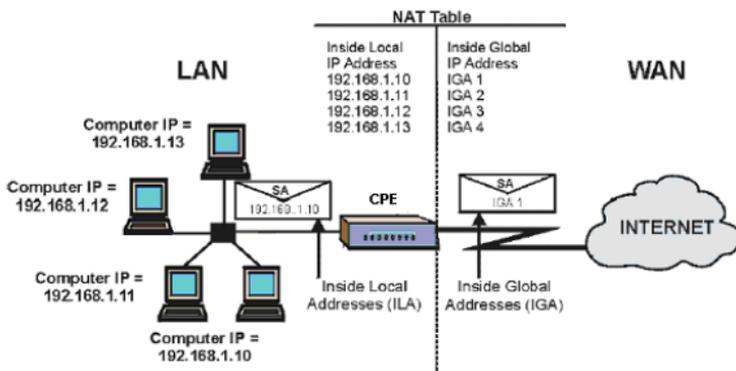
8.1.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP Alias) behind the ADSL Router can communicate with three distinct WAN networks. More examples follow at the end of this chapter.
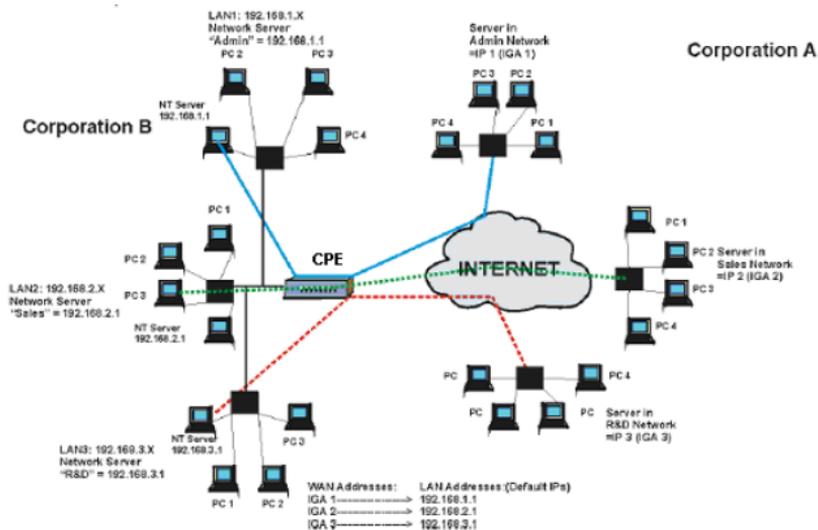
8.1.5 NAT Mapping Types

NAT supports five types of IP/port mapping. They are:

- **One to One:** In One-to-One mode, the ADSL Router maps one local IP address to one global IP address.
- **Many to One:** In Many-to-One mode, the ADSL Router maps multiple local IP addresses to one global IP address.
- **Many to Many Overload:** In Many-to-Many Overload mode, the ADSL Router maps the multiple local IP addresses to shared global IP addresses.
- **Many-to-Many No Overload:** In Many-to-Many No Overload mode, the ADSL Router maps each local IP address to a unique global IP address.
- **Server:** This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.

The following table summarizes these types:

Type	IP Mapping
One-to-One	ILA1 IGA1
Many-to-One (SUA/PAT)	ILA1 IGA1 ILA2 IGA1 ...
Many-to-Many Overload	ILA1 IGA1 ILA2 IGA2 ILA3 IGA1 ILA4 IGA2 ...
Many-to-Many No Overload	ILA1 IGA1 ILA2 IGA2 ILA3 IGA3 ...
Server	Server 1 IP IGA1 Server 2 IP IGA1 Server 3 IP IGA1

8.2 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a implementation of a subset of NAT that supports two types of mapping, Many-to-One and Server. The ADSL Router also supports Full Feature NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types as outlined in.

8.3 Virtual Server and DMZ

A Virtual server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though SUA makes your whole inside network appear as a single computer to the outside world.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for

example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

Default Server IP Address

In addition to the servers for specified services, NAT supports a default server IP address. A default server receives packets from ports that are not specified in this screen.

8.3.1 Port Forwarding: Services and Port Numbers

A NAT server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make accessible to the outside world even though NAT makes your whole inside network appear as a single machine to the outside world.

Use the SUA Server page to forward incoming service requests to the server(s) on your local network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers.

In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded. The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers.

| Application	Outcoming Connections	Incoming Connections
ICQ 98, 99a	Nessuno	Nessuno
NetMeeting 2.1 a 3.01	Nessuno	1503 TCP, 1720 TCP
VDO Live	Nessuno	Nessuno
mIRC	Nessuno	Nessuno
Cu-SeeMe	7648 TCP &UDP, 24032 UDP	7648 TCP &UDP, 24032

		UDP
PC AnyWhere	5632 UDP, 22 UDP, 5631 TCP, 65301 TCP	5632 UDP, 22 UDP, 5631 TCP, 65301 TCP
Edonkey/Emule	Nessuno	principalmente 4660-4662 TCP , 4665-4672 UDP
MSN Messanger	Nessuno	TCP da 6891-6900 TCP 1863 TCP 6901 UDP 1863 UDP 6901 UDP 5190
VNC	Nessuno	TCP 5900

Service	Port Number / Protocol
File Transfer Protocol (FTP) Data	20/tcp
FTP Commands	21/tcp
Telnet	23/tcp
Simple Mail Transfer Protocol (SMTP) Email	25/tcp
Domain Name Server (DNS)	53/tcp and 53/udp
Trivial File Transfer Protocol (TFTP)	69/udp
finger	79/tcp
World Wide Web (HTTP)	80/tcp
POP3 Email	110/tcp
SUN Remote Procedure Call (RPC)	111/udp
Network News Transfer Protocol (NNTP)	119/tcp
Network Time Protocol (NTP)	123/tcp and 123/udp
News	144/tcp
Simple Management Network Protocol (SNMP)	161/udp
SNMP (traps)	162/udp
Border Gateway Protocol (BGP)	179/tcp
Secure HTTP (HTTPS)	443/tcp

rlogin	513/tcp
rexec	514/tcp
talk	517/tcp and 517/udp
ntalk	518/tcp and 518/udp
Open Windows	2000/tcp and 2000/udp
Network File System (NFS)	2049/tcp
X11	6000/tcp and 6000/udp
Routing Information Protocol (RIP)	520/udp
Layer 2 Tunnelling Protocol (L2TP)	1701/udp

8.3.2 Virtual Server

Click on **Advanced Setup** then **NAT**.
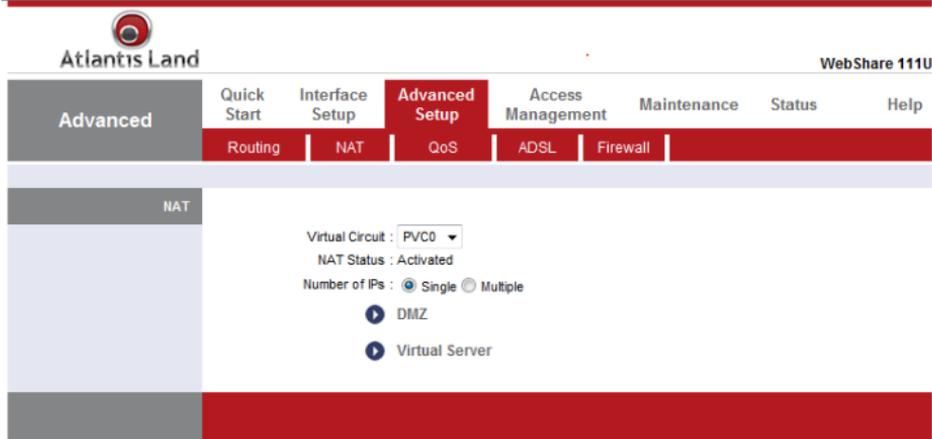
Click on **Virtual Server**.

Atlantis Land

Atlantis Land

WebShare 111U

Advanced	Quick Start	Interface Setup	Advanced Setup	Access Management	Maintenance	Status	Help

Routing	NAT	QoS	ADSL	Firewall	

Virtual Server

Virtual Server for : Single IP Account
Rule Index : 1
Application : -   -
Protocol : ALL
Start Port Number : 0
End Port Number : 0
Local IP Address : 0.0.0.0

Virtual Server Listing

Rule	Application	Protocol	Start Port	End Port	Local IP Address
1	-	-	0	0	0.0.0.0
2	-	-	0	0	0.0.0.0
3	-	-	0	0	0.0.0.0
4	-	-	0	0	0.0.0.0
5	-	-	0	0	0.0.0.0
6	-	-	0	0	0.0.0.0
7	-	-	0	0	0.0.0.0
8	-	-	0	0	0.0.0.0
9	-	-	0	0	0.0.0.0
10	-	-	0	0	0.0.0.0
11	-	-	0	0	0.0.0.0
12	-	-	0	0	0.0.0.0
13	-	-	0	0	0.0.0.0
14	-	-	0	0	0.0.0.0
15	-	-	0	0	0.0.0.0
16	-	-	0	0	0.0.0.0

SAVE   DELETE   BACK   CANCEL

The following table describes the labels in this screen:

| Field	Description
Start Port No.	Enter a port number in this field. To forward only one port, enter the port number again in the End

	Port No. field.
	To forward a series of ports, enter the start port number here and the end port number in the End Port No. field.
End Port No.	Enter a port number in this field.
	To forward only one port, enter the port number again in the Start Port No. field above and then enter it again in this field.
	To forward a series of ports, enter the last port number in a series that begins with the port number in the Start Port No. field above.
Local IP Address	Enter your server IP address in this field.

Let's say you want to assign ports 22-25 to one server, port 80 to another and assign a default server IP address of 192.168.1.35 as shown in the next figure.
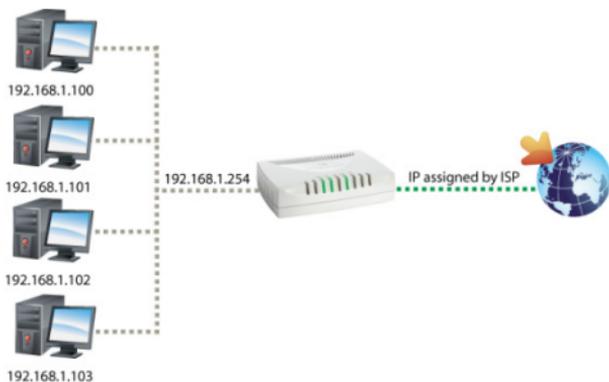
8.4 Selecting the NAT Mode

Click **Advanced Setup** then **NAT** to open the following screen chose **Multiple (Numbers of IP)**.
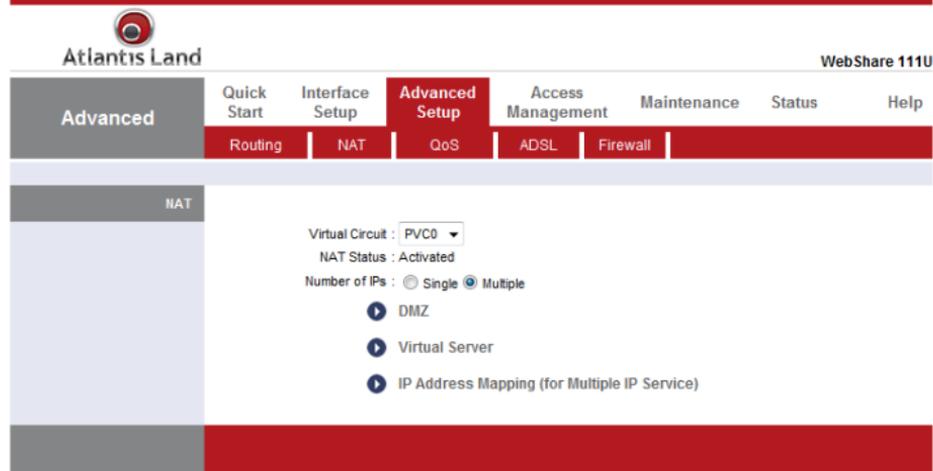
Click on **IP Address Mapping** (for Multiple IPs Service).

Atlantis Land   **WebShare 111U**

Advanced	Quick Start	Interface Setup	Advanced Setup	Access Management	Maintenance	Status	Help

Routing	NAT	QoS	ADSL	Firewall	

IP Address Mapping

Address Mapping Rule : PVC0
Rule Index : 1
Rule Type : One-to-One
Local Start IP : 0.0.0.0
Local End IP : N/A
Public Start IP : 0.0.0.0   (0.0.0.0 for modem's WAN IP)
Public End IP : N/A

Address Mapping List

Rule	Type	Local Start IP	Local End IP	Public Start IP	Public End IP
1	-	. . .	. . .	. . .	. . .
2	-	. . .	. . .	. . .	. . .
3	-	. . .	. . .	. . .	. . .
4	-	. . .	. . .	. . .	. . .
5	-	. . .	. . .	. . .	. . .
6	-	. . .	. . .	. . .	. . .
7	-	. . .	. . .	. . .	. . .
8	-	. . .	. . .	. . .	. . .

SAVE   DELETE   BACK   CANCEL

Ordering your rules is important because the ADSL Router applies the rules in the order that you specify. When a rule matches the current packet, the ADSL Router takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9. Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so old rules 5, 6 and 7 become new rules 4, 5 and 6.
To change the ADSL Router's address mapping settings.

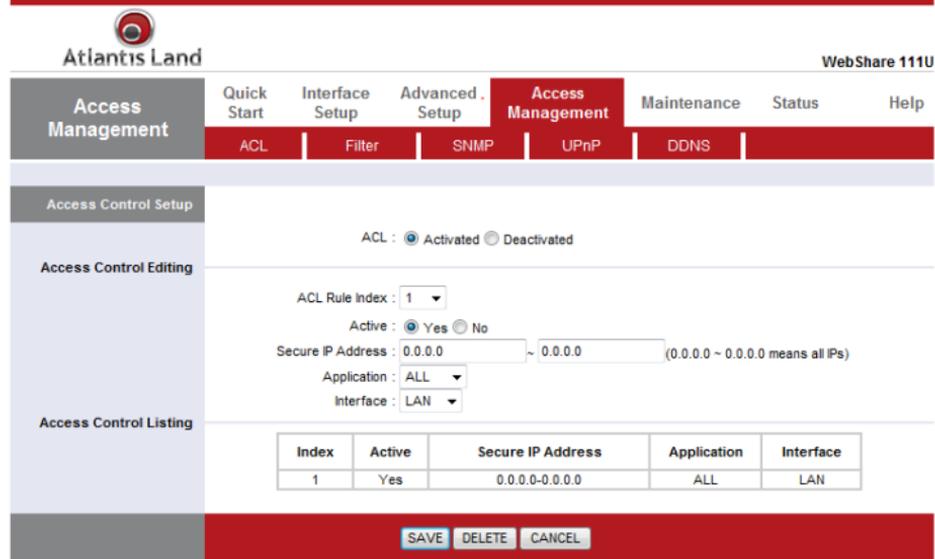The following table describes the labels in this screen:

Field	Descriptions
Rule Index	Choose the number
Rule Type	**1-1:** One-to-one mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type. **M-1:** Many-to-One mode maps multiple local IP addresses to one global IP address. **M-M Ov (Overload):** Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. **MM No (No Overload):** Many-to-Many No Overload mode maps each local IP address to unique global IP addresses. **Server(available on next release of firmware):** This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Local Start IP	This is the starting Inside Local IP Address (ILA). Local IP addresses are N/A for Server port mapping.
Local End IP	This is the end Inside Local IP Address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address. This field is N/A for One-to-one and Server mapping types.
Public Start IP	This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for Many-to-One and Server mapping types.
Public End IP	This is the ending Inside Global IP Address (IGA). This field is N/A for One-to-one, Many-to-One and Server mapping types.

9. Access Management

9.1 Access Control List (ACL)

Access Control Listing allows you to determine which services/protocols can access which WEBSHARE 111U interface from which computers.

You can configure the router for remote Telnet access or upload and download router firmware and configuration files using FTP. To use this feature, your computer must have an FTP client. And can use the WEBSHARE 111U embedded web configurator for configuration and file management.

Field	Meaning
ACL Rule Index	This is item number
Secure IP Address	The default 0.0.0.0 allows any client to use this service to remotely manage the WEBSHARE 111U. Type an IP address to restrict access to a client with a matching IP address

Application	Choose a service that you may use to remotely manage the WEBSHARE 111U.
Interface	Select the access interface. Choices are **LAN**, **WAN** and **Both**

9.2 Filter

In this section is possible to set different filtering type, based on IP/MAC, URL or Application.

9.2.1 IP/MAC Filter

Field	Description
IP Filter set Editing	
IP Filter set Index	This is item number
Interface	Select which channel (PVC) to configure
Direction	Select the access to the Internet ("Outgoing") or from the Internet ("Incoming") or Both
IP Filter Rule Editing	
IP Filter Rule Index	This is item number
Rule Type	Select Yes from the drop down list box to enable IP filter rule
Active	The source IP address or range of packets to be monitored
Source IP Address	It is the destination IP addresses based on above destination subnet IP
Subnet Mask (Source)	This Port or Port Ranges defines the port allowed to be used by the Remote/WAN to connect to the application. Default is set from range 0 ~ 65535. It is recommended that this option be configured by an advanced user
Port Number (Surce)	This is the destination subnet IP address
Destination IP Address	It is the destination IP addresses based on above destination subnet IP
Subnet Mask(destination)	It is the packet protocol type used by the application, select either TCP or UDP or ICMP
Port Number(destination)	Select action for the traffic unmatching current rule; Forward to leave it pass through, and NEXT to check it by the next rule
Protocol	This is item number
Rule Unmatched	Select Yes from the drop down list box to enable IP filter rule
IP Filter Listing	
#	Item number
Active	Whether the connection is currently activ
Source IP Mask	The source IP address or range of packets to be monitored
Destination IP Mask	This is the destination subnet IP address
Source port	This Port or Port Ranges defines the port allowed to be used by the Remote/WAN to connect to the application. Default is set from range 0 ~ 65535. It is recommended that this option

	be configured by an advanced user
Destination Port	This is the Port or Port Ranges that defines the application
Protocol	It is the packet protocol type used by the application, select either TCP or UDP or ICMP

9.2.2 Application Filter

Field	Meaning
Application Filter	Select this option to Activated/Deactivated the Application filter.
ICQ	Select this option to Allow/Deny ICQ.
MSN	Select this option to Allow/Deny MSN.
YMSG	Select this option to Allow/Deny Yahoo messenger.
Real Audio/Video	Select this option to Allow/Deny Real Audio/Video.

9.2.3 URL Filter

Field	Meaning
Active	Select **Active** to enable URL Filter.
URL Index	This is item number.
URL	Allow you to prevent users on your network from accessing particular websites by their URL.

9.3 SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. WebShare 111U supports SNMP agent functionality which allows a manager station to manage and monitor the router through the network.
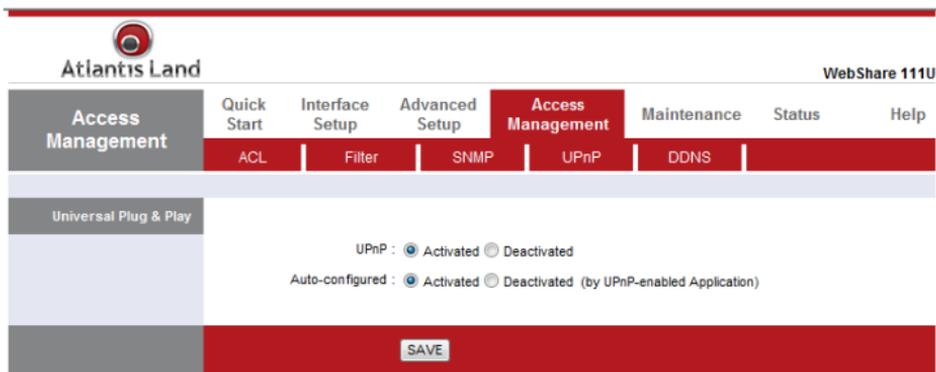

Field	Description
Get Community	Type the Get Community, which is the password for the incoming Get-and GetNext requests from the management station
Set Community	Type the Set Community, which is the password for incoming Set requests from the management station

9.4 UPnP

UPnP offers peer-to-peer network connectivity for PCs and other network devices, along with control and data transfer between devices. UPnP offers many advantages for users running NAT routers through UPnP NAT Traversal, and on supported systems makes tasks such as port forwarding much easier by letting the application control the required settings, removing the need for the user to control advanced configuration of their device.

Both the user's Operating System and the relevant application must support UPnP in addition to the router. Windows XP and Windows Me natively support UPnP (when the component is installed), and Windows 98 users may install the Internet Connection Sharing client from Windows XP in order to support UPnP. Windows 2000 does not support UPnP.

Field	Description
UPnP	Select this checkbox to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the WEBSHARE 111U IP address
Auto-configured	Select this check box to allow UPnP-enabled applications to automatically configure the WEBSHARE 111U so that they can communicate through the WEBSHARE 111U, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application

9.5 Dynamic DNS

The Dynamic DNS function allows you to alias a dynamic IP address to a static hostname, allowing users whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your ADSL connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP.
You will first need to register and establish an account with the Dynamic DNS provider using their website, for example http://www.dyndns.org/

Field	Description
Dynamic DNS	Select this check box to use dynamic DNS
Service Provider	Select the name of your Dynamic DNS service provider
Host Name	Type the domain name assigned to your WEBSHARE 111U by your Dynamic DNS provider
E-mail Address	Type your e-mail address

User	Type your user name
Password	Type the password assigned to you
Wildcard Support	Select this check box to enable DYNDNS Wildcard

10. Advanced Setup

This section will show how to configure static route, virtual server, Adsl line module and firewall.

10.1 Routing

If you have another router with a LAN-to-LAN connection, you may create a static routing on the router that is the gateway to Internet.

Field	Description
#	Item number
Dest IP	IP address of the destination network
Mask	The destination mask address
Gateway IP	IP address of the gateway or existing interface that this route uses

Metric	It represents the cost of transmission for routing purposes. The number need not be precise, but it must be between 1 and 15
Device	Media/channel selected to append the route
Use	Counter for access times
Edit	Edit the route; this icon is not shown for system default route
Drop	Edit the route; this icon is not shown for system default route

10.1.1 Add Route

Field	Meaning
Destination IP Address	This is the destination subnet IP address
IP Subnet Mask	It is the destination IP addresses based on above destination subnet IP
Gateway IP Address	This is the gateway IP address to which packets are to be forwarded
Metric	It represents the cost of transmission for routing purposes. The number need not be precise, but it must be between 1 and 15
Announced in RIP	This parameter determines if the Prestige will include the route to the remote node in its RIP broadcasts. Set "Yes", it is kept private and is not included in RIP broadcasts. Set "No", the remote node will be propagated to other hosts through RIP broadcasts

Advanced	Quick Start	Interface Setup	Advanced Setup	Access Management	Maintenance	Status	Help
	Routing	NAT	QoS	ADSL	Firewall		

Static Route	
Destination IP Address :	192.168.2.1
IP Subnet Mask :	255.255.255.0
Gateway IP Address :	◉ 192.168.1.200 ○ PVC0 ▾
Metric :	2
Announced in RIP :	No ▾

SAVE   DELETE   BACK   CANCEL

10.2 NAT

The NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet. The default setting is **Dynamic NAPT**. It provides dynamic Network Address Translation capability between LAN and multiple WAN connections, and the LAN traffic is routed to appropriate WAN connections based on the destination IP addresses and Route Table. This eliminates the need for the static NAT session configuration between multiple LAN clients and multiple WAN connections.

Field	Meaning
Virtual Circuit	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. There are eight groups of PVC can be defined and used
Number of IPs	User can select Single or Multiple

10.2.1 DMZ

The DMZ Host is a local computer exposed to the Internet. When setting a particular internal IP address as the DMZ Host, all incoming packets will be checked by the Firewall and NAT algorithms then passed to the DMZ host, when a packet received does not use a port number used by any other Virtual Server entries.

Field	Meaning
DMZ	**Disabled:** As set in default setting, it disables the DMZ function. **Enabled:** It activates your DMZ function.
DMZ Host Address	Give a static IP address to the DMZ Host when Enabled radio button is checked. Be aware that this IP will be exposed to the WAN/Internet.

10.3 Virtual Server

In TCP/IP and UDP networks a port is a 16-bit number used to identify which application program (usually a server) incoming connections should be delivered to. Some ports have numbers that are pre-assigned to them by the IANA (the Internet

Assigned Numbers Authority), and these are referred to as "well-known ports". Servers follow the well-known port assignments so clients can locate them.

If you wish to run a server on your network that can be accessed from the WAN (i.e. from other machines on the Internet that are outside your local network), or any application that can accept incoming connections (e.g. Peer-to-peer/P2P software such as instant messaging applications and P2P file-sharing applications) and are using NAT (Network Address Translation), then you will usually need to configure your router to forward these incoming connection attempts using specific ports to the PC on your network running the application. You will also need to use port forwarding if you want to host an online game server.

The reason for this is that when using NAT, your publicly accessible IP address will be used by and point to your router, which then needs to deliver all traffic to the private IP addresses used by your PCs. Please see the WAN configuration section of this manual for more information on NAT.

The device can be configured as a virtual server so that remote users accessing services such as Web or FTP services via the public (WAN) IP address can be automatically redirected to local servers in the LAN network. Depending on the requested service (TCP/UDP port number), the device redirects the external service request to the appropriate server within the LAN network.

Field	Meaning
Rule Index	Choose the rule number
Start Port Number	Enter a port number in this field
End Port Number	Enter a port number in this field
Local IP Address	Enter your server IP address in this field

10.4 IP Address Mapping

Field	Meaning
Rule Index	Choose the rule number
Rule Type	• **One-to-one:** This is the mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type • **Many-to-One:** This is the mode maps

	multiple local IP addresses to one global IP address. This is equivalent to Many to One (i.e., PAT, port address translation)
	• **Many-to-Many Overload:** This is mode maps multiple local IP addresses to shared global IP addresses
	• **Many-to-Many No Overload:** This is the mode maps each local IP address to unique global IP addresses
	• **Server:** This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Local Start IP	This is the starting Inside Local IP Address (ILA). Local IP addresses are N/A for Server port mapping
Local End IP	This is the end Inside Local IP Address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address. This field is N/A for One-to-one and Server mapping types
Public Start IP	This is the starting Inside Public IP Address. Enter 0.0.0.0 here if you have a dynamic IP address from your ISP
Public End IP	This is the ending Inside Public IP Address. This field is N/A for One-to-one, Many-to-One and Server mapping types

NOTE:

If you have disabled the NAT option in the WAN-ISP section, the Virtual Server function will hence be invalid.

If the DHCP server option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easiest way of configuring Virtual Servers is to manually assign static IP address to each virtual server PC, with an address that does not fall into the range of IP addresses that are to be issued by the DHCP server. You

can configure the virtual server IP address manually, but it must still be in the same subnet as the router.

10.5 QoS

Quality of Service (QoS) helps to prioritize data as it enters your router. By attaching special identification marks or headers to incoming packets, QoS determines which queue the packets enter, based on priority. This is useful when there are certain types of data you want to give higher priority to, such as voice data packets given higher priority than Web data packets.

The main goal of QoS is prioritizing incoming data, preventing data loss due to factors such as jitter, delay and dropping. Another important aspect of QoS is ensuring that prioritizing one data flow doesn't interfere with other data flows.

QoS can be toggled **Activated** and **Deactivated**. QoS must be activated before you can edit the following options. When you are done making changes, click on **Add** to save your changes.

Click on **QoS Settings Summary** to view the list of QoS rules that have been added.

The following table describes the labels in this screen:

Field	Descriptions
RULE	

Rule Index	Select 16 different rules, each rule's detail can be set and saved.
Active	Select QoS is activated or deactivated.
Application	Select 11 different applications: IGMP, SIP, H.323, MGCP, SNMP, DNS, DHCP, RIP, RSTP, RTCP, RTP.
Physical Port	Once you select the application, the associated ports will be displayed.
Destination MAC	Set the Ethernet MAC value that you want to filter in destination side.
Destination IP	Set the IP address value that you want to filter in destination side.
Destination Mask	Set the subnet mask value that you want to filter in destination side.
Destination Port Range	Set the port range value that you want to filter in destination side.
Source MAC	Set the Ethernet MAC value that you want to filter in source side.
Source IP	Set the IP address value that you want to filter in source side.
Source Mask	Set the subnet mask value that you want to filter in source side.
Source Port Range	Set the port range value that you want to filter in source side.
Protocol ID	Set the protocol ID type that you want to filter.
VLan ID Range	Set the Vlan value that you want to filter.
IPP/DS Field	Select IP QoS format.
IP Precedence Range	Select the IP precedence range.
Type of Service	Select 5 different type of service.
DSCP Range	Set the DSCP value that you want to filter.
802.1p	Set the remarked new 802.1p priority value on the packet that fulfill every detail setting condition of each rule.
<center>**ACTION**</center>	
IPP/DS Field	Select IP QoS format.
IP Precedente Remarking	Select the remarking value of IP precedence.
Type of Service Remarking	Select the remarking value of type of service.

DSCP Marking	Select the remarking value of DSCP.
802.1p Marking	Select the remarking value of 802.1p.
Queue#	Select four types of Queue: Low, Medium, High, Highest.

10.6 ADSL

Field	Description
ADSL Mode	The default setting is Auto Sync-UP. This mode will automatically detect your ADSL, ADSL2+, ADSL2, G.dmt, G.lite, and T1.413. But in some area, multimode cannot detect the ADSL line code well. If it is the case, please adjust the ADSL line code to G.dmt or T1.413 first. If it still fails, please try the other values such as ALCTL, ADI, etc
ADSL Type	There are five modes "Open Annex Type and Follow DSLAM's Setting", "Annex A", "Annex I", "Annex A/L", "Annex M" and "Annex A/I/L/M" that user can select for this connection

10.7 Firewall

In this section You can set Firewall and SPI protection on WebShare 111U.

11. Manteinance

11.1 Administration

In factory setting, the default password is atlantis, and that for user is also password. You can change the default password to ensure that someone cannot adjust your settings without your permission. Every time you change your password, please record the password and keep it at a safe place.

Field	Description
New Password	Type the new password in this field
Confirm Password	Type the new password again in this field

11.2 Time Zone

The router does not have a real time clock on board; instead, it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server outside your network. Choose your local time zone. After a successful connection to the Internet, the router will retrieve the correct local time from the SNTP server you have specified. If you prefer to specify an SNTP server other than those in the drop-down list, simply enter its IP address as shown above. Your ISP may provide an SNTP server for you to use.

Field	Description
Synchronize time with	Select the time service protocol that your time server sends when you turn on the Router

Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT)
Daylight Saving	Select this option if you use daylight savings time
NTP Server Address	Enter the IP address of your time server. Check with your ISP/network administrator if you are unsure of this information

11.3 Firmware

Your router's "firmware" is the software that allows it to operate and provides all its functionality. Think of your router as a dedicated computer, and the firmware as the software it runs. Over time this software may be improved and modified, and your router allows you to upgrade the software it runs to take advantage of these changes. To upgrade the firmware of WEBSHARE 111U, you should download or copy the firmware to your local environment first. Press the "**Browse…**" button to specify the path of the firmware file. Then, click "**Upgrade**" to start upgrading. When the procedure is completed, WEBSHARE 111U will reset automatically to make the new firmware work.

Field	Description
New Firmware Location	Type in the location of the file you want to upload in this field or click **Browse** to find it.
New RomFile Location	Romfile means the configuration file. Type in the location of the file you want to upload in this field or click Browse to find it.
Romfile Backup	Click **ROMFILE SAVE** button to save current configuration file to your PC.
Upgrade	Click **UPGRADE** to begin the upload process. This process may take up to two minutes.

After two minutes, log in again and check your new firmware version in the System Status screen.

If the upload was not successful, the following screen will appear. Click Back to go back to the Firmware screen.

Error Message:

ERROR: FAIL TO UPDATE DUE TO... The uploaded file was not accepted by the router.

Back

NOTE: DO NOT power down the router or interrupt the firmware upgrading while it is still in process. Improper operation could damage the router.

11.4 SysRestart

Click **SysRestart** with option **Current Settings** to reboot your router (and restore your last saved configuration).
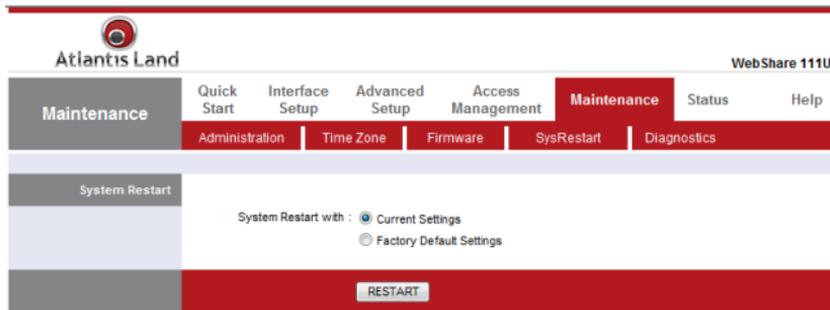
If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select **Factory Default Settings** to reset to factory default settings.
You may also reset your router to factory settings by holding the small Reset pinhole button on the back of your router in for 10-12 seconds whilst the router is turned on.

11.5 Diagnostic

The Diagnostic Test page shows the test results for the connectivity of the physical layer and protocol layer for both LAN and WAN sides.

12. Status

12.1 Device Info

Field	Description
Device Information	
F/W Version	This is the Firmware version
MAC Address	This is the MAC Address

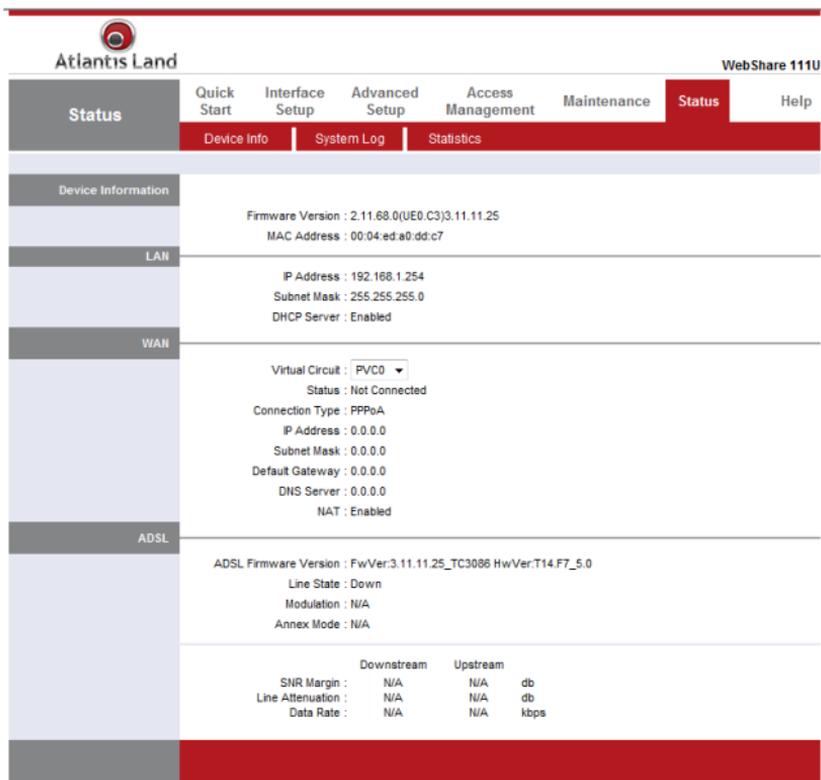| LAN Information	
IP Address	LAN port IP address
IP Subnet Mask	LAN port IP subnet mask
DHCP Server	LAN port DHCP role - Enabled, Relay or disabled
WAN Information	
Status	"Not connected" or "Connected"
Virtual Circuit	There are eight groups of PVC can be defined VPI: The valid range for the VPI is 0 to 255 VCI: The valid range for the VCI is 32 to 65535
Connection Type	Name of the WAN connection
IP Address	WAN port IP address
IP Subnet Mask	WAN port IP subnet mask
Default Gateway	The IP address of the default gateway
DNS	WAN port DHCP role - Enabled, Relay or disabled
NAT	Enabled or disabled
ADSL	
ADSL Firmware Version	This is the DSL firmware version associated with your router
Line State	This is the status of your ADSL link
Modulation	This field displays the ADSL modulation status for G.dmt or T1.413.
Annex mode	To show the router's type, e.g. Annex A, Annex B
SNR Margin	To show the router's SNR margin for Downstream/Upstream
Line Attenuation	To show the router's for Downstream/Upstream
Data Rate	To show the router's data rate for Downstream/Upstream

12.2 System Log

Display system logs accumulated up to the present time. You can trace historical information with this function.

12.3 Statistics

Read-only information here includes port status and packet specific statistics. Also provided are "Transmit Statistics" and "Receive Statistics".

ETHERNET	
Field	**Meaning**
Interface	This field displays the type of port
Transmit Frames	This field displays the number of frames transmitted in the last second
Transmit Multicast Frames	This field displays the number of multicast frames transmitted in the last second
Transmit total Bytes	This field displays the number of bytes transmitted in the last second
Transmit Collision	This is the number of collisions on this port
Transmit Error Frames	This field displays the number of error packets on this port
Receive Frames	This field displays the number of frames received in the last second
Receive Multicast Frames	This field displays the number of multicast frames received in the last second
Receive total Bytes	This field displays the number of bytes received in the last second
Receive CRC Errors	This field displays the number of error packets on this port
Receive Under-size Frames	This field displays the number of under-size frames received in the last second

ADSL	
Field	**Meaning**
Transmit total PDUs	This field displays the number of total PDU transmitted in the last secon
Transmit total Error Counts	This field displays the number of total error transmitted in the last second

Receive total PDUs	This field displays the number of total PDU received in the last second
Receive total Error Counts	This field displays the number of total error received in the last second

APPENDIX A: Troubleshooting

This chapter covers potential problems and the corresponding remedies.

A.1 Using LEDs to diagnose problems

The LEDs are useful aides for finding possible problem causes.

A.1.1 Power LED

The PWR LED on the front panel does not light up.

Steps	Corrective Action
1	Make sure that the ADSL Router's power adaptor is connected to the ADSL Router and plugged in to an appropriate power source. Use only the supplied power adaptor.
2	Check that the ADSL Router and the power source are both turned on and the ADSL Router is receiving sufficient power.
3	Turn the ADSL Router off and on.
4	If the error persists, you may have a hardware problem. In this case, you should contact your vendor.

A.1.2 LAN LED

The LAN LED on the front panel does not light up.

Steps	Corrective Action
1	Check the Ethernet cable connections between the ADSL Router and the computer or hub.
2	Check for faulty Ethernet cables.
3	Make sure your computer's Ethernet card is working properly.
4	If these steps fail to correct the problem, contact your local distributor for assistance.

A.1.3 ADSL LED

The DSL LED on the front panel does not light up.

Steps	Corrective Action
1	Check the telephone wire and connections between the ADSL Router DSL port and the wall jack.
2	Make sure that the telephone company has checked your phone line and set it up for DSL service.
3	Reset your ADSL line to reinitialize your link to the DSLAM. For details, refer to the Maintenance chapter (web configurator) or the System Information and Diagnosis chapter.
4	If these steps fail to correct the problem, contact your local distributor for assistance.

A.2 Telnet

I cannot telnet into the ADSL Router.

Steps	Corrective Action
1	Check the LAN port and the other Ethernet connections.
2	Make sure you are using the correct IP address of the ADSL Router. Check the IP address of the ADSL Router.
3	Ping the ADSL Router from your computer. If you cannot ping the ADSL Router, check the IP addresses of the ADSL Router and your computer. Make sure your computer is set to get a dynamic IP address; or if you want to use a static IP address on your computer, make sure that it is on the same subnet as the ADSL Router.
4	Make sure you entered the correct password. The default password is "admin". If you have forgot your username or password, refer to Section A.5.
5	If these steps fail to correct the problem, contact the distributor.

A.3 WEB Configurator

I cannot access the web configurator.

Steps	Corrective Action
1	Make sure you are using the correct IP address of the ADSL Router. Check the IP address of the ADSL Router.

	2	Make sure that there is not an console session running.
	3	Check that you have enabled web service access. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on remote management for details.
	4	For WAN access, you must configure remote management to allow server access from the Wan (or all).
	5	Your computer's and the ADSL Router's IP addresses must be on the same subnet for LAN access.
	6	If you changed the ADSL Router's LAN IP address, then enter the new one as the URL.
	7	Remove any filters in LAN or WAN that block web service.
	8	See also Section A.9.

The web configurator does not display properly.

Steps	Corrective Action
1	Make sure you are using Internet Explorer 5.0 and later versions.
2	Delete the temporary web files and log in again. In Internet Explorer, click Tools, Internet Options and then click the Delete Files ... button. When a Delete Files window displays, select Delete all offline content and click OK. (Steps may vary depending on the version of your Internet browser.)

A.4 Login Username e Password

I forgot my login username and/or password.

Steps	Corrective Action
1	If you have changed the password and have now forgotten it, you will need to upload the default configuration file. This will erase all custom configurations and restore all of the factory defaults including the password.
2	Press the RESET button for five seconds, and then release it. When the SYS LED begins to blink, the defaults have been restored and the ADSL Router restarts. Or refer to the Resetting the ADSL Router

	section for uploading a configuration file via console port.
3	The default username is "admin". The default password is "atlantis". The Password and Username fields are case-sensitive. Make sure that you enter the correct password and username using the proper casing.
4	It is highly recommended to change the default username and password. Make sure you store the username and password in a save place.

A.5 LAN Interface

I cannot access the ADSL Router from the LAN or ping any computer on the LAN.

Steps	Corrective Action
1	Check the Ethernet LEDs on the front panel. A LAN LED should be on if the port is connected to a computer or hub. If the 10M/100M LEDs on the front panel are both off, refer to Section A.1.2.
2	Make sure that the IP address and the subnet mask of the ADSL Router and your computer(s) are on the same subnet.

A.6 WAN Interface

Initialization of the ADSL connection failed.

Steps	Corrective Action
1	Check the cable connections between the ADSL port and the wall jack. The DSL LED on the front panel of the ADSL Router should be on.
2	Check that your VPI, VCI, type of encapsulation and type of multiplexing settings are the same as what you collected from your telephone company and ISP.
3	Restart the ADSL Router. If you still have problems, you may need to verify your VPI, VCI, type of encapsulation and type of multiplexing settings with the telephone company and ISP.

I cannot get a WAN IP address from the ISP.

Steps	Corrective Action
1	The ISP provides the WAN IP address after authenticating you.

	Authentication may be through the user name and password, the MAC address or the host name.
2	The username and password apply to PPPoE and PPoA encapsulation only. Make sure that you have entered the correct Service Type, User Name and Password (be sure to use the correct casing).

A.7 Internet Access

I cannot access the Internet.

Steps	Corrective Action
1	Make sure the ADSL Router is turned on and connected to the network.
2	If the DSL LED is off, refer to Section A.1.3.
3	Verify your WAN settings.
4	Make sure you entered the correct user name and password.

Internet connection disconnects.

Steps	Corrective Action
1	Check the schedule rules.
2	If you use PPPoA or PPPoE encapsulation, check the idle time-out setting.
3	Contact your ISP.

A.8 Remote Management

I cannot remotely manage the ADSL Router from the LAN or WAN.

Steps	Corrective Action
1	Refer to the Remote Management Limitations section in the Firmware and Configuration File Management chapter for scenarios when remote management may not be possible.
2	Use the ADSL Router's WAN IP address when configuring from the WAN. Use the ADSL Router's LAN IP address when configuring from the LAN.
3	Refer to Section A.6 for instructions on checking your LAN

	connection.
	Refer to Section A.7 for instructions on checking your WAN connection.
4	See also the Section A.4.

A.9 Remote Node Connection

I cannot connect to a remote node or ISP.

Steps	Corrective Action
1	Check WAN screen to verify that the username and password are entered properly.
2	Verify your login name and password for the remote node.
3	If these steps fail, you may need to verify your login and password with your ISP.

APPENDICE B: Technical Specifications

Protocols	IP, NAT, ARP, ICMP, IGMP, DHCP(server, client and relay), RIP1/2 , SNTP client, UPnP, Telnet server, SNMP
LAN Port	1 x RJ45 10/100 Base-T port
USB Port	1 porta USB v1.1
WAN Port	RJ-11 (1 port ADSL)
Button	Reset/Power Switch
LEDs	PWR, LAN, USB, ADSL, PPP
Standard ADSL Compliance	ANSI T1.413 Issue 2, ITU-T G.992.1(Full Rate DMT), ITU-T G.992.2 (Lite DMT), ITU-T G.994.1 (Multimode), ITU G.992.3 (G.dmt.bis), ITU G.992.5 (G.dmt.bisplus)
ADSL Encapsulation	RFC2364(PPPoA), RFC2516(PPPoE) e RFC1483 (Bridge and Routed)
ATM	ATM AAL2/AAL5 and ATM service class : CBR, UBR, VBR-rt, VBR, ATM Forum UNI 3.0, 3.1 and 4.0
Firewall	Packet Filtering (up to 72 rules) and NAT, URL Filtering
VPN	Pass Through
Power Supply (External)	12V AC @ 1A
Power Consumption	< 9watts
Compliant with	CE
Physical Dimensions	190mm x 120mm x 47mm
Weight	350g
Operative Temperature	Da 0° a 40° C
Storage Temperature	Da −10° a 70° C
Operative Humidity	5-95% no condensing

Atlantis Land

APPENDICE C: Support

If you have any problems with the WebShare 111U, please consult this manual. If you continue to have problems you should contact the dealer where you bought this ADSL Router. If you have any other questions you can contact the Atlantis Land company directly at the following address:

Atlantis Land
Via Pelizza da Volpedo, 59
20092 Cinisello Balsamo (MI) - Italy
Tel: +39. 02.00.632.300
Fax: +39. 02.66.016.666
Website: http://www.atlantis-land.com
Email: info@atlantis-land.com

Via Pelizza da Volpedo, 59
Cinisello Balsamo – MI – Italy
info@atlantis-land.com